REMARKS

Claims 1-6 and 22-31 have previously been canceled. New claims 41-46 have been added. Claims 7-21 and 32-46 are now pending in this application.

The Examiner is thanked for the in-person interview held August 14, 2008 with the undersigned and with Mr. Jubin Dana. During the interview, claim 7 was discussed and the Examiner suggested that an initial step of receiving authentication information regarding the customer during the registration process could lead to patentability of the claim. Applicant also agreed to file the present request for continued examination. Applicant requests a further in-person interview during the week of November 17, 2008.

Accordingly, independent claim 7 has been reintroduced as new independent claim 44 that includes an initial step where the authentication information of the customer is received at the access control server. New dependent claims 45 and 46 relate respectively to the embodiments where the issuer pre-loads this authentication information so that the customer does not have to go through a formal, online registration process, and where the customer does provide this authentication information during a formal registration process. Support may be found, for example, at pages 11-13; no new matter has been added. In addition, a new third step of "receiving an authentication request message" has been added to make clear that the third party is requesting verification of the identity of the customer during the online transaction.

Therefore, Applicant respectfully requests that new claims 44-46 are now in condition for allowance.

Rejections under Section 103

The final Office action dated March 21, 2008 has rejected claims 7-21 and 32-40 under section 103 as being unpatentable over *Barnes et al.* in view of *O'Mahony*, "Electronic Payment Systems" (*O'Mahony*). Although the Examiner's arguments have been carefully considered, Applicant respectfully traverses this rejection. Applicant has previously submitted detailed arguments in the amended appeal brief filed September 4, 2007 arguing for the patentability of claims 7-21 and 32-40, and Applicant stands by those arguments and submits that these claims are also in condition for allowance.

Dependent Claims

New dependent claims 41-43 have been added. Claim 41 requires that the authentication request message and the notifying message are routed via the browser of the customer computer; the advantage is that communication is quicker and a separate connection need not be established. Support is shown, for example, in Figure 6.

Claim 42 requires that once the customer has accessed the web site of the third party, that the customer browser is redirected to the web site of the access control server (for receiving the password), and then the browser is redirected back to third party web site. The advantage is that the authentication process is transparent to the customer and the customer receives the impression that he or she has not left the web site of the third-party merchant. Support may be found, for example, at pages 15 and 16.

Claim 43 requires that the step of requesting the password from the user does not require that any additional software relating to the authentication method be resident on the customer computer. The advantage is that participation in this authentication technique is simpler for the customer, thus promoting greater acceptance. Support may be found, for example, at page 9.

Linehan Reference (Patent No. 6,327,578)

During the interview, the Examiner raised the question of the relevance of the *Linehan* reference. In order to expedite prosecution, Applicant submits this analysis of that reference.

Linehan does not teach or suggest any registration process by which the identity of the customer is verified. Column 14 at lines 34-40 discuss a consumer presenting a password or smart card, but there is no disclosure of a registration process where the identity of the entity is verified. Claim 7 (for example) requires that the issuer verify the identity of the customer during a registration process. While *Linehan* does disclose using a password or other to authenticate the consumer, there is no guarantee that the issuer of *Linehan* has used any rigorous process to confirm that the consumer is actually who he says he is. Thus, the merchant of *Linehan* cannot receive any assurance that the consumer's identity has been verified. By contrast, claim 7 (for example), requires a verification of the customer's identity for the third party's benefit. *Linehan* discusses use of a password or perhaps a debit card and PIN; there is no guarantee that the customer has gone through a registration process where his or her identity has been verified. It is entirely possible that the issuer of *Linehan* simply accepts at face value the identity of the

consumer and then blindly issues a password or accepts a PIN without verifying the consumer's identity.

Linehan at column 9 discloses that an issuing bank may choose to authenticate a consumer using a password, cryptography, smart cards, etc. This disclosure only addresses how a consumer is authenticated during a transaction; for example, a consumer submits a password. But, this disclosure does not address how the consumer comes to be associated with a password in the first place. There is no discussion of any type of registration process during which the consumer's identity is *verified,* and then a password is assigned to that consumer. The only conclusion that can be drawn is that the consumer simply chooses a user name and password on their own; there is no disclosure of any *verification* taking place. Column 10 of *Linehan* only discusses that the issuing bank maintains a database that maps authorization numbers to card numbers. While this database helps identify which cards are associated with which authorizations, there is no disclosure of a registration process during which a consumer's identity is verified.

Claim 7 (for example) requires that the third party (such as an online merchant) send a request to the issuer requesting that the identity of the customer be authenticated. There is no disclosure in *Linehan* suggesting that the merchant is specifically requesting that this *authentication* take place. The merchant is certainly requesting an *authorization* for the transaction from the issuer (column 6, line 48-column 7, line 2), but the merchant is not requesting, nor does the merchant receive, an *authentication* of the cardholder. This result is not surprising as while the merchant certainly wishes to be paid, the merchant may not be too concerned about who exactly is paying it.

In addition, column 14 at lines 24-64 likewise discloses the *authorization* request and response between the merchant and the issuer, but do not disclose any specific *authentication* request and response. Column 14 refers only to the issuer verifying the merchant's digital signature, not receiving a request from the merchant to authenticate the identity of the consumer. Likewise, the disclosure at column 4 discusses the issuer verifying the merchant's digital signature. The disclosure at column 5 discusses a merchant message 222 but does not disclose any request from the merchant to *authenticate* the entity. Finally, column 7 of *Linehan* discloses a message from the merchant but there is no request for authentication.

The fifth "notifying" step above of claim 7 requires that the issuer notify the third party

online that the customer has been authenticated and that the customer is the owner of the account. Thus, in response to its request, the third party receives an assurance that the customer has been authenticated. Column 9 at lines 29-67 of *Linehan* discloses a request from the merchant for *authorization* and a response from the issuer regarding authorization, but there is no specific request for *authentication* of the cardholder from the merchant nor any specific acknowledgment from the issuer to the merchant that the cardholder has been *authenticated*, as specifically required by the above steps of claim 7. Column 14 at lines 40-54 only discuss "a signed *authorization* token" sent to the merchant; there is no indication to the merchant that the consumer has been *authenticated.*

Claim 41 requires that messages between the third party and the issuer are routed through an Internet browser of the customer. By contrast, Figure 1 of *Linehan* shows that messages are not routed via the consumer; Figure 4 shows that the request message 402 and the response token 402' are not routed via the consumer. Even though Figures 2, 5 and 6 show messages passing through the consumer computer 202, these messages are being handled by the consumer wallet software, and not by the Internet browser of the consumer. (See column 9, lines 34-67 of *Linehan*). The disadvantage of the approach of *Linehan* is that extra consumer wallet software must be installed and maintained on the consumer computer. Claim 41 is simpler and does not require extra software.

Claim 43 requires that no additional software is needed on the customer computer in order to implement the authentication method. *Linehan* makes quite clear that extra consumer wallet software is required. For example, Figure 3 at steps 306 and 312, and Figure 8 at 814 disclose use of the wallet software. Further, the following portions of *Linehan* disclose that the extra wallet software is required: column 2, lines 17-31 and 66-67; column 4, lines 9-23; column 5, lines 63-67; column 9, lines 41-46; column 10, lines 13-32; column 13, lines 31-47; column 14, lines 33-39 and 65-67; and column 15, lines 55-58. The portion at column 14, lines 65-67 makes clear that consumer wallet software is separate because when it terminates, normal browsing proceeds with the browser software.

Claim 42 requires that a customer's browser is redirected to an access control server of the issuer to perform authentication, and then redirected back to the third-party web site. This feature is not disclosed in *Linehan*.

Reconsideration of this application and issuance of a Notice of Allowance at an early date are respectfully requested. If the Examiner believes a telephone conference would in any way expedite prosecution, please do not hesitate to telephone the undersigned at (612) 252-3330.

Respectfully submitted,
BEYER LAW GROUP LLP

/Jonathan O. Scott/

Jonathan O. Scott
Registration No. 39,364

BEYER LAW GROUP LLP
P.O. Box 1687
Cupertino, CA 95015-1687

Telephone: (612) 252-3330
Facsimile: (612) 825-6304